IN THE CLAIMS:

1-15. (Cancelled)

16. (Original) A file encryption apparatus that encrypts a plaintext to generate a ciphertext and stores the ciphertext into a memory unit thereof, the file management apparatus comprising:

a key storage medium storing key information beforehand;

registration means for receiving an input of a password, encrypts the key information using the received password to generate an encrypted key, and writes the generated encrypted key to the memory unit; and

encryption unit means for encrypting a plaintext using a file key to generate a ciphertext, encrypting the file key using the key information to generate an encrypted file key, and writing the ciphertext in association with the encrypted file key, to the memory unit.

17. (Original) A file decryption apparatus that stores the ciphertext and the encrypted file key generated by the file encryption apparatus of Claim 16, in association with each other, in a memory unit thereof, and decrypts the ciphertext, the file decryption apparatus comprising:

a key storage medium storing key information beforehand:

switch means

(a) including first key obtaining means for receiving an input of a password and decrypting the encrypted key using the received password to generate key information, and second key obtaining means for reading the key information from the key storage medium, and

(b) obtaining the key information by one of the first key obtaining means and the second key obtaining means; and

decryption means for decrypting the encrypted file key using the obtained key information to generate a file key, and decrypts the ciphertext using the file key to generate a decrypted text.

18-43. (Cancelled)

Please add the following newly drafted Claims 44-60.

44. (New) The file encryption apparatus of Claim 16, wherein the registration means further receives an input of a user identifier that identifies a user, and writes the user identifier in association with the encrypted key, to the memory unit.

45. (New) The file encryption apparatus of Claim 16, wherein the registration means further writes the key information and/or authentication information in association with the encrypted key, to the memory unit,

the encryption means further writes the encrypted key, the key information, and/or authentication information in association with the ciphertext, to the memory unit.

46. (New) The file encryption apparatus of Claim 16, wherein the registration means writes the encrypted key to the memory unit that is a portable storage medium.

47. (New) The file encryption apparatus of Claim 16, further comprising:

deletion means for deleting the encrypted key that has been written to the memory unit.

48. (New) The file encryption apparatus of Claim 16, further comprising:

deletion means for deleting the encrypted key that has been written to the memory unit,

wherein the registration means further receives an input of a new password, encrypts the key information using the new password to generate a new encrypted key, and writes the generated new encrypted key to the memory unit.

49. (New) The file encryption apparatus of Claim 16, wherein the key storage medium stores new key information beforehand, instead of the key information,

the registration means receives the input of the password and decrypts the encrypted key using the password to generate key information,

the encryption means decrypts the encrypted file key using the key information to generate a file key, encrypts the file key using the new key information to generate a new encrypted file key, and writes the new encrypted file key over the encrypted file key in the memory unit, and

the registration means encrypts the new key information using the password to generate a new encrypted key and writes the new encrypted key over the encrypted key in the memory unit.

50. (New) The file encryption apparatus of Claim 49, wherein the registration means further receives an input of a user identifier that identifies a user,

the encryption means further writes the user identifier in association with the ciphertext and the encrypted file key, to the memory unit, and

the encryption means retrieves the encrypted file key that is associated with the user identifier in the memory unit and generates a file key from the retrieved encrypted file key.

51. (New) The file encryption apparatus of Claim 49, wherein the encryption means further writes encryption information in association with the ciphertext and the encrypted file key, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption means retrieves the encrypted file key that is associated with the encryption information in the memory unit, and generates a file key from the retrieved encrypted file key.

52. (New) The file encryption apparatus of Claim 49, wherein the registration means further receives an input of a user identifier that identifies a user,

the encryption means further writes the user identifier in association with a file identifier that identifies the ciphertext and the encrypted file key, as a unified file, to the memory unit, and

the encryption means extracts the file identifier that is associated with the user identifier from the unified file, specifies the encrypted file key identified by the extracted file identifier, and generates a file key from the specified encrypted file key.

53. (New) The file encryption apparatus of Claim 49, wherein the encryption means further writes encryption information in association with a file identifier that identifies the ciphertext and the encrypted file key, as a unified file, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and the encryption means extracts the file identifier that is associated with the encryption information from the unified file, specifies the encrypted file key identified by the extracted file identifier, and generates a file key from the specified encrypted file key.

54. (New) The file encryption apparatus of Claim 16, wherein the encryption means further writes the encrypted key in association with the ciphertext and the encrypted file key, to the memory unit.

55. (New) The file encryption apparatus of Claim 54, wherein the encryption means further receives an input of an indication, the indication showing whether the encrypted key and the ciphertext are to be written in association with each other to the memory unit, and writes, when the indication shows that the encrypted key and the ciphertext are to be written in association with each other, the encrypted key in association with the ciphertext, to the memory unit.

56. (New) The file encryption apparatus of Claim 54, wherein the registration means writes the generated encrypted key to the key storage medium instead of to the memory unit.

57. (New) The file decryption apparatus of Claim 17, wherein the file encryption apparatus further receives an input of a user identifier that identifies a user, and writes the user identifier in association with the encrypted key, to the memory unit, and

the first key obtaining means further receives an input of the user identifier and decrypts the encrypted key that is associated with the user identifier.

58. (New) The file decryption apparatus of Claim 17, wherein the file encryption apparatus further writes the key information and/or authentication information in association with the encrypted key, to the memory unit, and further writes the encrypted key, the key information, and/or authentication information in association with the ciphertext, to the memory unit,

the first key obtaining means checks, using the authentication information, whether the encrypted key has been altered or not, when the encrypted key that is associated with the authentication information is decrypted, and the decryption means checks, using the authentication information, whether the ciphertext has been altered or not, when the ciphertext that is associated with the authentication information is decrypted.

59. (New) The file decryption apparatus of Claim 17, wherein the file encryption apparatus writes the encrypted key to the memory unit that is a portable storage medium, and

the first key obtaining means decrypts the encrypted key that has been written to the memory unit that is the portable storage medium.

60. (New) The file decryption apparatus of Claim 17,

wherein the file encryption apparatus further writes the encrypted key in association with the ciphertext and the encrypted file key, to the memory unit, and

the first key obtaining means decrypts the encrypted key that is associated with the ciphertext and the encrypted file key.